Deutscher Bundestag **Drucksache 19/9086**
19. Wahlperiode 05.04.2019

Kleine Anfrage

der Abgeordneten Andrej Hunko, Heike Hänsel, Anke Domscheit-Berg, Dr. André Hahn, Ulla Jelpke, Thomas Nord, Petra Pau, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

Attribuierung von „böswilligen Cyberaktivitäten“ durch das geheimdienstliche EU-Lagezentrum INTCEN

Der Rat der Europäischen Union hat beschlossen, eine „Cyber Diplomacy Toolbox“ für eine gemeinsame Reaktion der EU auf „böswillige Cyberaktivitäten“ zu entwickeln (Ratsdokument 9916/17). Der Cyberraum bringe Herausforderungen auch für die Gemeinsame Außen- und Sicherheitspolitik mit sich. So sei es „mehr und mehr notwendig“, die Integrität und Sicherheit der EU, ihrer Mitgliedstaaten sowie ihrer Bürgerinnen und Bürger „vor Bedrohungen aus dem Cyberraum und böswilligen Cyberaktivitäten zu schützen“.

Ein gemeinsamer umfassender Ansatz der EU für die Cyberdiplomatie soll auch die „Eindämmung von Cyberbedrohungen“ besorgen. Dabei geht es auch um die Attribuierung von Störungen oder Angriffen im Cyberraum. Hierzu soll unter anderem das geheimdienstliche EU-Lagezentrum INTCEN Erkenntnisse beisteuern, sammeln und bewerten (Ratsdokument 6852/19). Das EU-INTCEN soll außerdem bei der Entscheidungsfindung für eine mögliche Reaktion auf „böswillige Cyberaktivitäten“ mitarbeiten. Dies ist jedoch aus Sicht der Fragestellerinnen und Fragesteller mit den EU-Verträgen unvereinbar, denn diese sehen keine Kompetenz für die Koordination der Geheimdienste vor. Auch eine nichtbindende Einschätzung des EU-INTCEN zu möglichen Reaktionen wäre kritisch, da Mitgliedstaaten dadurch im Sinne anderer Geheimdienste, die über mehr Aufklärungsfähigkeiten verfügen und Erkenntnisse bewusst an das INTCEN steuern, beeinflusst werden könnten.

Wir fragen die Bundesregierung:

1. Wie definiert die Bundesregierung „böswillige Cyberaktivitäten“, und inwiefern wird dabei auch zwischen staatlichen und nichtstaatlichen Akteuren unterschieden (vgl. Ratsdokument 7298/19)?
2. Hat die Bundesregierung jemals einen terroristischen Cyberangriff zweifelsfrei oder mit einer hohen Wahrscheinlichkeit attribuiert?
3. Welche Akteure und Einrichtungen der Europäischen Union sollten aus Sicht der Bundesregierung bei der Attribuierung „böswilliger Cyberaktivitäten“ Erkenntnisse beisteuern, und mit welchen Einschränkungen soll dies auch für das geheimdienstliche EU-Lagezentrum INTCEN gelten?
4. Sollte das EU-INTCEN aus Sicht der Bundesregierung auch dann aktiv werden, wenn nur ein einzelner EU-Mitgliedstaat von „böswilligen Cyberaktivitäten“ betroffen ist?

5. Welche Akteure und Einrichtungen der Europäischen Union sollten aus Sicht der Bundesregierung Vorschläge für eine Reaktion auf „böswillige Cyberaktivitäten“ machen, und mit welchen Einschränkungen soll dies auch für das EU-INTCEN gelten?
6. Welche einzelnen Aspekte „böswilliger Cyberaktivitäten“ sollte das EU-INTCEN aus Sicht der Bundesregierung vorrangig bewerten (etwa Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung; vgl. Ratsdokument 9916/17)?
7. Welche technischen Mittel könnte die Europäische Union aus Sicht der Bundesregierung zur Attribuierung „böswilliger Cyberaktivitäten“ beisteuern (bitte auch die verantwortlichen Agenturen nennen)?
8. Nach welchem Verfahren könnte das EU-INTCEN aus Sicht der Bundesregierung bewerten, mit welcher Wahrscheinlichkeit „böswillige Cyberaktivitäten“ tatsächlich einem bestimmten Akteur zugeordnet werden können (etwa das im Ratsdokument 7298/19 aufgeführte Verfahren, das von weniger als 5 Prozent bis hin zu mehr als 95 Prozent reicht)?
9. Welche eigenen, nicht von Geheimdiensten der EU-Mitgliedstaaten gelieferten Erkenntnisse sollte das EU-INTCEN aus Sicht der Bundesregierung für die Attribuierung „böswilliger Cyberaktivitäten“ nutzen?
10. In welchem Umfang haben die Geheimdienste des Bundes in den letzten zwei Jahren im Rahmen ihrer jeweiligen gesetzlichen Vorschriften für die EU-Ebene relevante Erkenntnisse zu „böswilligen Cyberaktivitäten“ an das EU-INTCEN bzw. die dort angesiedelte EU-Analyseeinheit für hybride Bedrohungen („Hybrid Fusion Cell“) geliefert (Bundestagsdrucksache 19/7881, Antwort zu Frage 18)?
11. Inwiefern arbeitet das EU-INTCEN nach Kenntnis der Bundesregierung auch mit Geheimdiensten aus Drittstaaten zusammen, und um welche handelt es sich dabei?
12. Inwiefern sollten Mitgliedstaaten der Europäischen Union aus Sicht der Bundesregierung angehalten oder gedrängt werden, Erkenntnisse zur Attribuierung „böswilliger Cyberaktivitäten“ auf EU-Ebene oder gegenüber dem EU-INTCEN offenzulegen?
13. Inwiefern soll das INTCEN nach Kenntnis der Bundesregierung auch mit dem „internen Netz zur Abwehr von Desinformation“ der Generaldirektion Kommunikation (DG-COMM) der Europäischen Kommission zusammenarbeiten bzw. zuarbeiten, in dem Vertreterinnen und Vertreter aller Generaldirektionen sowie der Mitgliedstaaten organisiert sind (Bundestagsdrucksache 19/7881, Antwort zu Frage 12)?
14. Welche deutschen Einrichtungen sollen nach Kenntnis der Bundesregierung nach gegenwärtigem Stand mit dem EU-INTCEN zur Attribuierung „böswilliger Cyberaktivitäten“ kooperieren?
15. Mit wie vielen Mitarbeiterinnen und Mitarbeitern welcher Behörden ist die Bundesregierung am INTCEN und dem EUMS INT Directorate beteiligt (Bundestagsdrucksache 18/146, Antwort zu Frage 12)?
16. Welche Technik nutzen das INTCEN und das EUMS INT nach Kenntnis der Bundesregierung zur „Krisenfrüherkennung“ (vgl. Bundestagsdrucksache 19/7604)?
17. Wann soll das „Frühwarnsystem“ der Steuerungsgruppe Strategische Kommunikation im Auswärtigen Amt fertiggestellt bzw. betriebsbereit sein (Bundestagsdrucksache 19/7881, Antwort zu Frage 19)?

18. Welche Akteure und Einrichtungen der Europäischen Union könnten aus Sicht der Bundesregierung eine gemeinsame Attribuierung „böswilliger Cyberaktivitäten“ koordinieren?
    a) Wo sollte analysiert und bewertet werden, welche Konsequenzen eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten“ für die EU-Außenbeziehungen hat?
    b) Wo sollte analysiert und bewertet werden, inwiefern eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten“ die Arbeit der einbezogenen Agenturen und Einrichtungen der Europäischen Union behindert oder gefährdet?
    c) Wo sollte analysiert und bewertet werden, ob eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten“ mögliche Gegenmaßnahmen provozieren und einen Konflikt damit eskalieren könnte?
19. Welche Aufgaben sollte ein „Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung“ oder ein „Netz nationaler Koordinierungszentren“ aus Sicht der Bundesregierung bei der Attribuierung „böswilliger Cyberaktivitäten“ und einer gemeinsamen EU-Antwort übernehmen (Kommissionsdokument COM(2018) 630 final)?
20. Welche Haltung vertritt die Bundesregierung zur Frage, das „Rapid-Alert-System“ gegen „Desinformationskampagnen“ und „ausländische Beeinflussung“ von Wahlen für andere Organisationen (etwa NATO, G7) und Drittstaaten zu öffnen (http://gleft.de/2JYw), und auf welche Weise sollen auch Firmen (etwa Facebook, Google) eingebunden werden?
21. Zu welchen Themen hat die Plattform der geheimdienstlichen „Counter Terrorism Group“ (CTG) in Den Haag nach Kenntnis der Bundesregierung seit ihrem Bestehen Analysen erstellt, und an welchen dieser Arbeiten hat das Bundesamt für Verfassungsschutz aktiv mitgewirkt?
22. In welchen Fällen „böswilliger Cyberaktivitäten“ sollten aus Sicht der Bundesregierung die Regierungen der Mitgliedstaaten allein oder bilateral über mögliche Reaktionen entscheiden, und in welchen Fällen sollte dies als gemeinsame Antwort der Europäischen Union erfolgen?
23. Sollte die Europäische Union aus Sicht der Bundesregierung auch dann eine gemeinsame EU-Antwort auf „böswillige Cyberaktivitäten“ erwägen, wenn sie von einem Drittstaat hierzu aufgefordert wurde?
24. Inwiefern hat sich das EU-INTCEN nach Kenntnis der Bundesregierung mit der Sicherheit von 5G-Netzen befasst, und welche Empfehlungen wurden in diesem Zusammenhang ausgesprochen?
25. Was ist der Bundesregierung über die weiteren Pläne oder Diskussionen zum Aufbau einer „Geheimdienstakademie“ in Frankreich bekannt (Bundestagsdrucksache 19/8193, Frage 17)?
    a) Wie wird sich die Bundesregierung bei der Gestaltung der Einrichtung einbringen und welche ihrer Geheimdienste arbeiten daran mit?
    b) Welche weiteren Geheimdienste sollen für den Aufbau einer „Geheimdienstakademie“ eingebunden werden?

26. Welche Aspekte eines „gemeinsamen strategischen Verständnisses“ sollten aus Sicht der Bundesregierung im Vordergrund einer engeren Kooperation europäischer Geheimdienste stehen (Bundestagsdrucksache 19/8193, Frage 17, abweichende Version der vorläufigen Beantwortung: http://gleft.de/2JL)?

Berlin, den 20. März 2019

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333